



## **INITIAL DRAFT OUTLINE**

# **ENTERPRISE RESOURCE PLANNING SECURITY TECHNICAL IMPLEMENTATION GUIDE**

Version 1, Release 0

15 March 2006

**Developed by DISA for the DoD**

UNCLASSIFIED

This page is intentionally left blank.

## TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Background.....	1
1.2 Authority.....	2
1.3 Scope.....	2
1.4 Writing Conventions.....	3
1.5 Vulnerability Severity Code Definitions .....	3
1.6 DISA Information Assurance Vulnerability Management (IAVM).....	3
1.7 STIG Distribution .....	4
1.8 Document Revisions .....	4
<b>2. Enterprise Resource Planning Overview.....</b>	<b>1</b>
2.1 Introduction.....	1
2.2 ERP Processing Models.....	1
2.2.1 Two-Tier Model.....	2
2.2.2 Three-Tier Model.....	2
2.3 ERP Security approach .....	3
2.3.1 Development and Production Environments .....	3
<b>3. ERP General Security Requirements.....</b>	<b>5</b>
3.1 System Requirements.....	5
3.2 Network Requirements .....	6
3.3 Database Requirements.....	6
3.3.1 Database Userids/Accounts .....	6
3.4 Installation Requirements .....	6
3.4.1 System Delivered Userids/Accounts.....	7
3.4.2 Application File Protection.....	7
3.4.3 Implementation Project Controls .....	8
3.5 Application Access Controls.....	8
3.5.1 Developer Access.....	10
3.5.2 User Access.....	12
3.6 Password Guidelines.....	13
3.7 Special Considerations for Applications with Tightly Interconnected Production and Development Environments.....	14
3.8 Application Design Features.....	15
3.8.1 Remote Access to ERP Applications.....	15
3.9 Logging.....	15
3.10 Data Protection.....	15
3.10.1 At Rest .....	16
3.10.2 In transit – Network connections to the application .....	17
3.11 Application Access to System Services.....	18
3.12 Application Access to Database Services .....	18
3.12.1 Separation of user interface from data storage .....	18
3.13 Application Configuration and Customization Requirements.....	19
3.14 Patching and Maintenance Requirements.....	19

---

3.15	Audit .....	20
3.16	Backup .....	22
APPENDIX A. RELATED PUBLICATIONS.....		23
APPENDIX B. GLOSSARY OF TERMS.....		25
APPENDIX C. LIST OF ACRONYMS .....		27

## 1. INTRODUCTION

This Enterprise Resource Planning (ERP) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements and implementation details for Commercial-Off-The Shelf (COTS) ERP application software. For this STIG, Enterprise Resource Planning software will refer to all commercially available software packages that supply one or more of the functions generally found within ERP packages. The functions include but are not limited to Human Resources, Financial processes, Customer Relations Management (CRM), sales, warehousing, inventory control, and manufacturing.

This Enterprise Resource Planning (ERP) Security Technical Implementation Guide (STIG) provides security configuration guidance for software products designed to deliver enterprise-class system ERP functionality. While the boundaries of the ERP discipline are such that there is no authoritative definition of an ERP product, Section 2, Enterprise Resource Planning Overview, provides a generic description of the elements characteristic of most ERP products. Section 3, ERP General Security Requirements, provides general guidance for ERP products. In future versions of this STIG, specific commercial products are to be addressed in appendices.

This document is intended to be used in conjunction with the other STIGs developed by the Defense Information Systems Agency (DISA). The operating system (OS) STIGs provide crucial guidance for securing the platforms on which the ESM products run. The STIGs that cover database, networking, and web server products provide guidance to ensure those services used by ERP products also support a secure environment.

### 1.1 Background

For many years, ERP products have been used by business to standardize and integrate their business processes. These products helped to implement new regulatory compliance requirements, changes in business processing standards, and better leverage business information while freeing up corporate resources from the complexities of data processing so that they could focus on their core business competencies.

DoD is now deploying ERP systems to manage personnel processes and accounting/financial applications throughout its infrastructure. Though there are some aspects of ERP functionality that the DoD cannot use, the modularity of the available packages allows for the purchasing of only the functionality needed. As with commercial businesses, the use of ERP provides the DoD with better regulatory compliance and better use of current business “best practices”, while freeing up resources which can then be applied to mission critical projects.

From the perspective of security, ERP products are immature. ERP products evolved from mainframe based accounting and human resource applications, where they depended upon monolithic mainframe architecture and closed proprietary networks for security, into distributed server based applications on open networks, and lacking the implied security imposed from the legacy architectures. While this transformation was taking place, little thought was given to adding security. As open networking grew into the Internet these applications were exposed to more threats from both inside and outside the organization deploying ERP. To combat these new threats security was grafted onto the ERP applications and vendors gave more guidance on

isolating the ERP application, and its associated servers, from the organizational network, allowing only restricted access into the network segment supporting ERP. Though these initiatives mitigate the external threat, the internal security controls within the application and its associated servers remained weak leaving the application vulnerable to exploitation if an attack succeeds in breaching the security perimeter. Additionally because of the privileges granted the application in accessing system services a compromised application leaves the enclave network vulnerable to an internal attack if additional mitigating controls are not in place.

The goal of this document is to provide guidance that allows the power of ERP products to be utilized, while preventing that power from being exploited to degrade the confidentiality, integrity, or availability of the data under the control of the product.. It should be noted that Field Security Operations (FSO) support for the STIGs, Checklists, and Tools is only available to DoD Customers.

## **1.2 Authority**

DoD Directive 8500.1 requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DoD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

## **1.3 Scope**

This document describes security requirements to be applied to ERP products used in DoD environments. The information is designed to assist Security Managers, Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with the creation of more secure ERP configurations. As noted in the previous section, application of the requirements is intended to provide a certain level of assurance. Individual sites must determine if this level of assurance is appropriate to their environment.

This document provides general security guidance. Vendor implementation of ERP functionality does vary; and most commercial products provide only subsets of all the functions generally associated with ERP.

Future versions of this STIG will provide specific guidance for the following:

- SAP ERP
- PeopleSoft ERP (or the Oracle product that combines PeopleSoft with Oracle’s ERP products)

## 1.4 Writing Conventions

Throughout this document, statements are written using words such as “**will**” and “**should**.” The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses “**will**” indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all “**will**” statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to “**should**” indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item, for example, “(*G111: CAT II*).” If the item does not have a Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and “N/A” for the SDID (i.e., “*[N/A: CAT III]*”).

## 1.5 Vulnerability Severity Code Definitions

<b>Category I</b>	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
<b>Category II</b>	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
<b>Category III</b>	Vulnerabilities that provide information that potentially could lead to compromise.
<b>Category IV</b>	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

**Table 1.1. Vulnerability Severity Code Definitions**

## 1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, <http://www.cert.mil>.

## **1.7 STIG Distribution**

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is <http://iase.disa.mil/>.

## **1.8 Document Revisions**

Comments or proposed revisions to this document should be sent via e-mail to [fso\\_spt@disa.mil](mailto:fso_spt@disa.mil). DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.



## **2. ENTERPRISE RESOURCE PLANNING OVERVIEW**

Enterprise Resource Planning is a term used to describe a class of software that implements and integrates the business processes normally found in a business environment. By optimizing business processes and encapsulating them into logical modules, ERP software allows an organization to leverage their data and integrate their business processes to better fulfill their primary function. Benefits include faster financial close (resulting in more timely knowledge of financial results), timelier billing and receivables processing, more efficient accounts payable, optimized operations, and improved forecasting and planning.

### **2.1 Introduction**

ERP systems consist of functional modules that support business requirements such as Human Resources, Financials, or Inventory Control. The modules can be used individually or in conjunction with other modules as needed. The individual modules contain the business processes necessary to complete their intended function. These software processes need to be reconciled to the business processes used by the implementing organization. The organizational business processes may be modified to better fit with the ERP software (business process re-engineering), or the software may be tailored to the organization's processes. This tailoring is done by modifying the configuration of the module (by use of configuration tables) with little or no modification of the underlying code supplied by the vendor. Additionally the ERP packages all have a means of modifying the information displayed and stored within the system to match the requirements of the implementer. Though industry specific modules can be purchased is always required.

ERP packages contain utilities to assist in the tailoring of the modules. Often the packages contain a development environment where the system is configured, and interfaces developed to other Automated Information Systems (AIS) used within the organization.

If modifications are made to the underlying ERP source code to tailor the ERP to the business process of the organization, problems may arise when upgrading the ERP release level or applying vendor patches. This can lead to a loss of functionality in production or during upgrade preparation.

The data used by all modules is stored in a database. The database tables overlap where the module functionality overlaps to facilitate the process flow between. Though this is useful for business process efficiency it does lead to security concerns in that a user must have access to parts of a table within the database without necessarily having a need to access the whole table. A simple example of this would be a warehouse shift supervisor would need to know the home phone number for an on call employee. This information can be retrieved from the personnel table stored in the HR modules. However, these records also contain information that the supervisor does not need access to and should not be granted access.

### **2.2 ERP Processing Models**

ERP systems are often deployed in either two-tier (client/server) or three-tier (client/application server/database server) implementations.

### **2.2.1 Two-Tier Model**

In a two-tier model the server holds the database and database software. The business processes, the programs, are downloaded to the client and executed on the client's system and the client system fetches the data from the database server. Access to control is maintained by the business logic executing on the client system.

Some advantages of the two-tier model:

- The cost savings on server hardware.
- Expansion of the number of clients does not create a server bottleneck because the business process code is executing on the client systems.

Some disadvantages of the two-tier model:

- Increased network load.
- Data may be transferred to the client system that the user may not be authorized to view. Though the business logic will not allow the data to be displayed, the data is available on the client system and could be compromised.
- The database server must be visible to the client systems exposing it to additional vulnerabilities.
- Security auditing is difficult.

### **2.2.2 Three-Tier Model**

In a three-tier model the client uses a browser or thick client (graphical user interface) to access the application server. The business processes, the programs, are executed on the application server and fetch the data from the database server. Access control is maintained by the business process logic executing on the application server.

Some advantages of the three-tier model:

- Decreased network load.
- Scalable
- No data is transferred to the client system that the user is not authorized to access
- The database server needs to be visible only to the application server decreasing its exposure to vulnerabilities.
- Security auditing is centralized and simpler.

Some disadvantages of the three-tier model:

- Increased server cost (additional server need for the application server).
- Increase in usage can create a server bottleneck at the application server. This may require additional hardware to be purchased for additional application servers and load balancing hardware/software to balance the load between the multiple parallel application servers.

## **2.3 ERP Security approach**

ERP applications generally depend upon access controls enforced by the application code rather than operating system access controls or database access controls. Though they may have provisions for using third party or network authentication, in their native mode, they depend upon application code to authenticate the users (who could potentially be using weak passwords). To further enhance security the ERP applications depend upon a strong perimeter defense between the ERP servers and rest of the enclave network.

These applications usually execute under the control of one or more system privileged accounts. All of their database accesses are made via a single database administrator account that owns all ERP objects within the database.

### **2.3.1 Development and Production Environments**

Many ERP applications have a release control and management mechanism implemented within their design. This mechanism normally consists of a development environment, a Quality Assurance (QA) environment, and a production environment or some combination of these environments.

The development environments are used during the initial implementation project, as well as for development of enhancements and follow up modules. It is also used to test patches and updates from the vendor and major new releases of the ERP application. Table configuration settings are made in the development system to custom tailor the ERP application to the needs of the organization. Programming for additional system functionality and reports takes place here, and custom interfaces to existing applications are created. The developer prior to release for Quality Assurance testing performs unit testing of new functionality and code.

The QA environment is used to perform functional integration testing to assure that the ERP configuration and code perform as designed, without injecting new vulnerabilities or instabilities into the base ERP application. QA should reflect the production environment as closely as possible. The integration testing is normally performed by dedicated QA personnel and subject matter experts, to avoid bias introduced into the process by the developers. This testing should be thorough and should be done without privileged access in order to verify that the correct access levels are being granted to the end users. All aspects should be tested including functionality, documentation, and security.

If the application does not pass QA testing it is returned to the development environment for correction. No modifications are made to the configuration or code in the QA environment. When the corrections have been made the application is returned to the QA environment for thorough testing. Unit testing is not normally performed in the QA system, although occasionally the lack of adequate data in the development system will require that the QA system be used. In any case, after unit testing of changes is done, it must be followed by QA (integration) testing.

When the application or changes have successfully completed QA testing, the Configuration Control Board will approve them for production release. Once the production release is approved the application is moved to the production environment.

Since the movement of an application from testing to QA and finally to production can be a complex process, many ERP packages have a component to assist and control the process. These packages often require that the production environment be connected to the development and QA environments via a network connection. Care should be taken when designing and implementing these network connections to isolate the development environment from the production environment.

This isolation should ensure end users do not mistakenly access the test environment compromising test data with real data and processing test data as if it were real. Additionally the production environment needs to be protected so that development, unit testing and QA integration testing do not occur in the production environment compromising production data.

### 3. ERP GENERAL SECURITY REQUIREMENTS

This document takes into consideration the Sarbanes-Oxley Act of 2002 (SOX), specifically in the areas of segregation of duties and access to sensitive or powerful transactions, and the Health Insurance Portability and Accountability Act (HIPPA), particularly in the area of privacy. However, this document does not fully address these issues and is not intended to do so.

ERP User Roles and responsibilities within ERP systems are:

- IAO – Responsible for implementing and maintaining user and access security on the ERP system.
- IAM – Responsible for management and oversight of all ERP Information systems.
- ERP Administrator – (Also known as Basis for an SAP implementation) is responsible for maintaining the ERP internal configuration and tables and to keep the systems operating at peak efficiency.
- System Administrator (SA) – Responsible for the system on which the ERP application resides.
- Developer – Programmer responsible for ERP system customization, developing reports and writing interfaces for ERP applications.
- User – Refers to functional users who have responsibility for a specific functional module within the ERP system such as finance, materials management, human resources, etc.
- Data Base Administrator (DBA) – Responsible for maintaining the database(s) for the ERP application.

Access and privileges are assigned to users based on a collection of transactions and authorization objects, which grant permissions to each field in the object. Examples of fields are activities (read only, write, execute, etc), organizational units (plant, company code, organization), document type (purchase order, invoice, general ledger), and a plethora of other variables. An object might grant write access to factory 046 for warehousing receiving actions. Proper use of these security tools allows user access to be customized to their specific business needs. The permissions needed to perform a specific task or job are combined into security roles. Specific roles should be designed and granted to users on a need to know (“least privilege”) basis.

Some vendors use a security schema, which is based on “row level” security, but the principals involved are the same.

#### 3.1 System Requirements

It is imperative that system security requirements are set up in such a way that the integrity of the application remains strong. ERP application integrity depends on properly managing the overall

processing environment, including the ERP application, the network and operating system, the database, and the user workstation (OS patches, anti-spyware and virus detection programs, password protected screen savers). Proper system management helps to protect system hardware, software and application data from unauthorized access and improper modification or disclosure of sensitive information.

- *(ERP000700: N/A) The System Administrator will ensure the host systems are compliant with host OS STIG.*

### **3.2 Network Requirements**

ERP systems applications depend on network security to prevent inappropriate exposure of resources, which could circumvent application controls. Therefore the network will be designed and configured to be compliant with the Network Infrastructure STIG. Some ERP applications will not function properly if not configured to vendor specifications; therefore, consideration must be given to the ERP vendor's network security recommendations. If unable to comply with the Network STIG due to ERP software requirements a DAA extension will be required.

- *(ERP000705: N/A) The System Administrator will ensure the host network are compliant with Network Infrastructure STIG*

### **3.3 Database Requirements**

A layered approach to overall application security provides the highest level of security. Therefore the databases are compliant with the Database STIG, to protect the ERP as well as database UserID/ Accounts that are stored in the database.

- *(ERP000710: N/A) The DBA will ensure the database(s) associated with ERP applications are compliant with the Database STIG.*

#### **3.3.1 Database Userids/Accounts**

Because the ERP application requires elevated privileges for a single userid to perform all database access for the application, the database will not be shared with any other application. This will limit any unauthorized access solely to data within the ERP application should the ERP database user ID be compromised.

- *(ERP000720: N/A) The DBA will ensure elevated privileges for a single userid to perform all database functions are not shared with any other application.*

### **3.4 Installation Requirements**

Application integrity is most vulnerable to intrusion before applications have been completely configured for secure operation. Vendor delivered software has inherent vulnerabilities that need to be addressed during installation and prior to connection to the production network. Because of this vulnerability the application will not be connected to the network before security directives presented in this STIG are in place. System parameters, which reside in files at the operating system level, will be set before the ERP system is started

ERP systems typically provide numerous parameters and table settings, which govern security aspects of system behavior:

- Password length
- Password- required digits, letters, or special characters
- Prohibited passwords or phrases (commonly used or easily guessed)
- Number of incorrect login attempts before session ends or user ID is locked
- Auto unlock (does the system automatically unlock the ID at midnight?)
- Multi logins permitted?
- Use of previous passwords
- Length of time between mandatory password changes
- Inactive time before auto logoff
- Single sign on parameters
- Ticket parameters (including cache)

- *(ERP000735: N/A) The IAO and ERP Administrator will ensure system parameters which reside in operating system file are correctly set before the ERP is started*

### **3.4.1 System Delivered Userids/Accounts**

Since applications are delivered containing Userids and accounts that have well known default passwords, malicious users can make use of these accounts and userids unless action is taken prior to deployment. Vendor delivered Userids will be removed or passwords changed to non-trivial passwords.

- *(ERP000900: N/A)(Industry & DoD) The IAO will ensure the removal of system delivered user accounts or the changing of their passwords to generated passwords before moving the application to production.*
- *ERP000910: N/A) The IAO will ensure system parameters, which govern the auto-regeneration of user accounts (for example, SAP\*) are set so that the system does not regenerate the account automatically (with well-known password).*
- *(ERP000915: N/A) The IAO will ensure the removal of vendor delivered default PKI certificates.*

### **3.4.2 Application File Protection**

Since the application is not designed to be accessed other than through its own interfaces, and to protect the integrity of the application, all files installed with the application, used by the application and/or created by the application will be protected from system level access or modification by unauthorized system users.

Security objects within the application will be set to deny access at the operating system level. If some level of directory access is needed (for example, the uploading of spreadsheet data files),

directory access will be limited solely to the needed data directory, and with minimal read/write access. Additional security transactions and objects may govern access to execute operating system commands

Checks may include the means to limit access to transactions, administrative functions (ability to execute operating systems command may require an administrative object as well as a transaction), and dataset (directory access).

- *(ERP001210: N/A) (Industry) The IAO and ERP Administrator will ensure all files installed with the application, used by the application and/or created by the application are protected from system level access or modification by unauthorized system users with access controls appropriate to the host operating system.*

### 3.4.3 Implementation Project Controls

ERP application modifications can change the security posture impacting the confidentiality, integrity and availability of the application. A process of review mitigates potential vulnerabilities created by the changes.

- *(ERP001500: N/A)(Industry) IAO and ERP Administrator will ensure system changes are reviewed and approved by the CCB prior to implementation to verify that they do not compromise the security of the system.*

ERP systems have separate environments for development, testing and production. Each environment is configured with progressively restrictive controls. Only appropriate personnel will have access to each environment. During implementation controls are in place by correctly configuring the application to reflect the final production environment.

- *(ERP001510: N/A) (DoD) The IAO will ensure during deployment the ERP security controls reflect the intended production environment.*

### 3.5 Application Access Controls

This section identifies the discretionary access controls for identification and authentication criteria necessary to ensure access to ERP resources are effectively managed and controlled for ERP systems.

Documentation is key to consistent security measures being applied across an environment or an enterprise. Roles, responsibilities and security access authorizations will be clearly documented. Each user group should be aware of their specific roles and their responsibilities to protect data.

- *(ERP001900: N/A) (Industry) The IAO will ensure security controls, requirements, responsibilities, and procedures are documented.*

Controls will be in place to support segregation of duties for security, application administration, and development and user access.



- *(ERP002100: N/A) (DoD) The IAO will ensure application role based access control enforces separation of duties*

All available layers of security control will be utilized to form a layered “defense in depth”. This includes limiting both transaction and security object access for a given function. For example, loose control at the object level will not be permitted based on the assumption that the user will not have access to the transaction.

In addition, the following security authorization tools will be used

Assignment of user ID into user groups

Authorization to run programs

Authorization to view/ update tables

Batch administrator authorizations

- *(ERP002110: N/A) The IAO will ensure all available security control mechanisms are utilized in a layered defense*

Controls will be in place to ensure that security administration access is only assigned to the IAO. Access to the security software or access control mechanism of a system could allow security controls to be overridden. Access restricted to the IAO ensures that the security controls remain as intended.

- *(ERP002300: N/A)(Industry) The IAO will ensure access to the mechanism, which provides the system’s access control is restricted to those responsible for administering security for that system.*
- *(ERP002400: N/A) (Industry) The IAO will ensure the ability to change a users group membership is restricted to authorized security administrators.*

Access will be granted on a need-to-know basis (least privilege) and must be approved by the information owner or governing authority. Excessive access could allow a user to perform abusive or unauthorized acts, or commit errors that could result in unauthorized disclosure, modification or destruction of data. Excessive access also raises risk levels should a user’s account and password be compromised due to social engineering, weak password, or computer virus (Trojan horse keystroke logging program).

Modules for ERP applications are, for example, Human Resources (HR) Materials Management (MM), Financial (FI) etc.

A classification guide will exist for the ERP application to further detail the sensitivity of data in each of the ERP application modules.

- *(ERP002500: N/A) (Industry) The IAO will ensure access to information, assets and resources are only granted to users to support only their organization or module.*

- *(ERP002600: N/A)(DoD) The IAM will ensure a classification guide exists for the application.*

When a new employee requests access to an ERP system, the HR Department will set the employee up with a personnel number for identification purposes. This standard ensures user accountability. By verifying the identity of a user attempting to gain access, this ensures access is granted to the intended user.

There will be a documented procedure for unlocking users and changing passwords. Users must provide proof of identity before reactivation of the userid can occur.

- *(ERP002700: N/A) (Industry) The IAO will ensure each user is assigned a personal identifier to use in order to get passwords reset and accounts unlocked. Users produce proof of identify before reactivation occurs.*

Userids will not remain active on the system longer than necessary. This ensures that these userids will be unusable and not available for unauthorized users to log on.

- *(ERP002800: N/A)(DoD) The IAO will ensure userids are disabled after 60 days of inactivity and removed after 120 days of inactivity. (Industry Standard).*

To protect the integrity of the application, authorizations will be modified from the installation defaults in order to tightly control access. All User Access Roles (authorizations) should be created and managed in accordance with security policy and with SOX and HIPPA Audit controls in mind.

- *(ERP001300: N/A) (DoD) The IAO will customize all roles/authorizations to assign “least privilege” to all fields, taking into consideration SOX and HIPPA regulatory recommendations.*

Vendor delivered security roles, which are often presented as models, are often designed with ease/speed of implementation taking preference over best security practice. While these roles may be used as a reference, the authorizations must be reviewed and scaled down to least privilege. Over reliance on vendor models is a common mistake made in ERP implementations

- *(ERP001310: N/A)(Industry) The IAO will ensure vendor delivered roles are not be used.*

### **3.5.1 Developer Access**

In typical ERP installations there is usually a master configuration system, a Quality Assurance (QA) test system, and the production system. The master configuration system contains master copies of the ERP configuration and program source code. There is normally little or no data in the configuration master. Program development and new configuration take place in this system. The QA environment is used for integration testing of code and configuration changes, and should be very similar (or identical) to the production environment.

ERP applications provide a control mechanism to move changes to QA for end user testing and then to production after testing are complete and test cases are signed off. Access to the vehicle that moves these changes will be tightly controlled. Developers will not have the security permissions necessary to transport their own changes to production. The ERP production application will be set to “on-modifiable” so that configuration and program changes cannot be made directly there.

Developer access should be restricted to development and testing areas only. If necessary a developer may have read-only access to production in order to check their changes. Change control will be used to advance any changes to the production system and will include the approval of a Change Control Board (CCB) and Management. Developer’s will access ERP Development and Test systems with a unique userid and password. This prevents an unauthorized user from writing code, promoting to production and then executing the code without any approval, checks or balances.

Developers will not have authorization to run code in debug mode in production. Debug mode provides the capability to step through program code, potentially stepping over security authorization checks.

Additionally, advanced privileges granted to facilitate development present another avenue for the compromise of the application once development is complete. Failure to remove these privileges could result in authorized disclosure, modification or loss of production information by someone exploiting userids with these privileges.

- *(ERP001000: N/A) (Industry) The ERP Administrator and IAO will review all system changes and customization prior to implementation in production to ensure they do not compromise the security of the system.*
- *(ERP001100: N/A) (Industry) The IAO will remove any advanced privileges granted to developers during installation before moving the application to production.*
- *(ERP001200: N/A) (Industry) The ERP Administrator will ensure testing of all software or services have been completed in the test environment before moving the application to production.*
- *(ERP003000: N/A) (Industry) The IAO will ensure developers y have only userids in development and test areas of an ERP application with possibly read-only access in production if absolutely necessary.*
- *(ERP003100: N/A) (Industry) The CCB will review and approve all changes before advancing said changes into the production system.*
- *(ERP003110: N/A) (Industry) The AIO and ERP Administrator will ensure developers do not have the ability to run programs in debug mode in the production system.*

### 3.5.2 User Access

There will be unique identification in place for each system user. A user is either an individual or an executing process/service that accesses a computer resource. Actions performed by a user within the application will be traceable to an individual user account. Failure to implement this practice can compromise the integrity of data and eliminate the usefulness of audit trails.

- *(ERP003200: N/A) (DoD) The IAO will configure all ERP accounts to be protected by strong, non-default passwords.*
- *(ERP003300: N/A) (DoD) The IAO will ensure application userids are unique.*
- *(ERP003400: N/A)(Industry) The IAO will ensure information such as name and related access information is associated with each userid.*
- *(ERP003500: N/A) (Industry) The IAO will ensure all critical user actions are traceable to individual userids.*
- *(ERP003600: N/A) (Industry) ERP Administrator will configure the system to have userids disabled due to invalid password attempts. The userid is reactivated after positive verification of the user's identity has been obtained.*
- *(ERP003610: N/A) (Industry) The ERP Administrator will configure system settings in such a way that if a new userid is not logged on for 30 days that the userid will be disabled.*
- *(ERP003700: N/A) (DoD) The IAO will ensure non-privileged users will not be able to perform privileged functions.*
- *(ERP003900: N/A) (DoD) The ERP Administrator and the IAO will ensure the application will enable an application client to authenticate to the application server with which it communicates.*

PKI will be used in ERP applications, in order to validate a user's authentication. Password protection alone is not a strong enough mechanism, as it is too easy to break into applications where only passwords are used for authentication.

- *(ERP004000: N/A) (DoD) The IAM will ensure PKI will be used for authentication.*
- *(ERP004100: N/A) (DoD) The IAO will ensure MAC I applications only accept DoD Class 4 certificates resident on tokens. MAC II and MAC III applications may accept either DoD Class 3 or Class 4 certifications resident either on tokens or on the local disk.*
- *(ERP004200: N/A) (DoD) The IAO will ensure the ERP Application do not honor invalid certificates.*

- *(ERP004300: N/A) (DoD) The ERP Administrator and the IAO will ensure the application users cannot circumvent the intended user interface to access resources in its supporting infrastructure.*

Users should only have access to an application for as long as they are actively using the application. Session limits will be in place to time out the session after a specified time of inactivity occurs. This must be done to ensure no person other than the assigned user is using the user's session.

- *(ERP004400: N/A) (DoD) The ERP Administrator and IAO will ensure session limits exist for the application.*

A written requirement should be in place stating that the IAO be notified immediately when an employee leaves employment and their userid should be disabled as soon as notification occurs.

### **3.6 Password Guidelines**

Passwords must be protected from being accessed by unauthorized users. When an account is created for a user, that user must be given a temporary password. The IAO will brief the user on implementation of password protection.

- *(ERP004600: N/A) (DoD) The IAO will ensure user account passwords conform to DoD password policy and each user is briefed on the policy upon receiving a temporary password.*

All passwords will be stored in an encrypted format. The application account name and password will not be visible to the host or client operating system.

- *(ERP004500: N/A) The IAO will ensure user account passwords are stored in an encrypted format using FIPS 140-2 compliant encryption, NIST Certified cryptography or NSA approved cryptography.*

Application account logons should be limited to three failed logons before they become locked. This requirement reduces the ability for password cracking programs to be used successfully. The IAO will set the duration of the lock time to a specific length as approved by the IAO for the application or site or require a manual reset. The duration should be set appropriately for the environment, keeping in mind that the longer the duration, the more protected the accounts will be from password cracking programs. Passwords will be complex in nature to ensure they will not be easily guessable.

- *(ERP004700: N/A) (DoD) The IAO and ERP administrator will ensure ERP passwords are a minimum of eight characters and system parameters is set to enforce same.*
- *(ERP004800: N/A)(DoD) The IAO will notify users that account passwords do not contain personal information such as names, telephone numbers, account names, dictionary words, etc.*

- *(ERP004900: N/A)(DoD) The IAO will instruct users that account passwords do not contain consecutively repeating characters and system parameters are set to enforce same.*
- *(ERP005000: N/A)(DoD) The IAO will instruct users that account passwords differ from the previous five passwords and system parameters are set to enforce same.*
- *(ERP005100: N/A) (DoD) The IAO will ensure user account passwords expire every 90 days and system parameters are set to enforce same.*
- *(ERP005200: N/A) (DoD) The IAO will ensure user account passwords have at least one non-alphanumeric character (special) character, one number.*
- *(ERP005300: N/A) (DoD) The IAO will ensure users are not allowed to change their user account passwords more than once every 24 hours without IAO approval. System parameters are set to enforce same.*
- *(ERP005400: N/A) (DoD) The IAO will limit user account logons to three consecutive failed logons before the user account becomes locked and the IAO are called to reset the password after the user presents proof of identity. System parameters and written process are in place to enforce same.*

### **3.7 Special Considerations for Applications with Tightly Interconnected Production and Development Environments**

Production, test, and development environments should all be separate. Development must take place in the development environment then moved to the test environment to be tested for functionality and user tested. Changes should then be approved by the Configuration Control Board (CCB) and moved to the production environment by a different individual who has that designated function. A strict change control process will be in place and followed without exception.

- *(ERP005500: N/A)(DoD) The ERP Administrator will ensure all changes to production software, hardware, and communication links are managed through a change control process.*
- *(ERP005600: N/A) (Industry) The IAO will ensure modifications to systems and networks are evaluated for impact to security controls.*
- *(ERP005800: N/A) (Industry) The ERP Administrator and IAO will ensure user acceptance testing is performed and user sign-offs are obtained before changes are moved into production.*
- *(ERP005900: N/A) (DoD) The ERP Administrator will ensure the application environment does not use unnecessary services or software within the environment.*

- *(ERP006100: N/A) (Industry) The ERP Administrator and the IAO will ensure a documented process is in place to ensure unnecessary custom code is not included into a release. This would include program code reviews.*
- *(ERP006200: N/A) (DoD) The ERP Administrator will ensure application processes run with only privileges necessary for proper operation. This includes background user ID's needed by 3<sup>rd</sup> party "bolt on" products.*
- *(ERP006210: N/A) The ERP Administrator will ensure that although the test and development environments may reside on the same server, the production environment reside on a separate server.*

### **3.8 Application Design Features**

#### **3.8.1 Remote Access to ERP Applications**

All remote connections to the ERP systems by administrative users to perform administrative functions including application account password resets and account management will be encrypted in order to remove the possibility of using the credentials for an attack.

- *(ERP006300: N/A) (DoD) The IAO will ensure user account passwords are stored in an encrypted format using FIPS 140-2 compliant encryption, NIST Certified cryptography, or NSA approved cryptography depending on the classification of the data residing within the application.*
- *(ERP006400: N/A)(DoD) The IAO will ensure all administrative connections to the application are encrypted using FIPS 140-2 compliant encryption, NIST Certified cryptograph, or NSA approved cryptography depending on the classification of the data residing within the application.*
- *(ERP006500: N/A) (DoD) The IAO will ensure all remote user access to the application be encrypted using FIPS 140-2 compliant encryption, NIST Certified cryptography or NSA approved cryptography depending on the classification of the data residing within the application.*

### **3.9 Logging**

Reviews should be performed on application Logs a minimum of once a week. The purpose of these reviews is to ensure no one is attempting to gain unauthorized access by guessing passwords and that any unauthorized transaction attempts are mistakes and not malicious.

### **3.10 Data Protection**

Data is protected by strict controls of user userids and data access roles, which are assigned to users. The roles are maintained at the field level and are granted levels such as read, write, delete, etc. for particular modules of the application. Data classified as sensitive data by the data owner will be encrypted to protect from unauthorized viewing.

Field level checks (user input) will be performed to check for allowed input in order to protect the data integrity.

Both printed and application data should be protected in order to maintain confidentiality and integrity of the data. Procedures will be in place to mark printed material with sensitivity level if it does not appear on the report.

- *(ERP006700: N/A) (Industry) The IAO will ensure user procedures exist for manually marking printed documents if the printed report does not contain same.*
- *(ERP006800: N/A) (DoD) The ERP Administrator will ensure the application adequately validates user inputs before processing them.*
- *(ERP006900: N/A) (DoD) The ERP Administrator will ensure the application displays an appropriate warning message upon user logon.*
- *(ERP007000: N/A) (DoD) The IAO will ensure an application user or client authentication is adequate.*
- *(ERP0070100: N/A) (Industry) The IAO and ERP Administrator will ensure sensitive data is encrypted using FIPS 140-2 compliant encryption, NIST Certified cryptography or NSA approved cryptography depending on the classification of the data residing within the application.*

### **3.10.1 At Rest**

Data “at rest” will reside inside the server. First line of defense is the Operating System and the ERP application will be protected by normal ERP User Authorization and file protection standards indicated in the paragraph above. Data determined sensitive by the data owner may require encryption to protect against unauthorized viewing.

- *(ERP007100: N/A) The System Administrator and ERP Administrator will ensure if required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information.*
- *(ERP007200: N/A) The System Administrator and ERP Administrator will ensure if required by the information owner, NIST-certified cryptography is used to encrypt stored classified non-SAMI information.*
- *(ERP007300: N/A) The System Administrator and ERP Administrator will ensure if a classified enclave contains SAMI and is accessed by individuals lacking an appropriate clearance for SAMI, then NSA-approved cryptography is used to encrypt all SAMI stored within the enclave.*

Sensitive application data will be adequately protected at rest in order to prevent compromised data.



- *(ERP007400: N/A) (Industry) The ERP Administrator will ensure no user or process are able to write to any file containing keys. If keys need to be replaced or added, permissions are changed temporarily for those events.*
- *(ERP007500: N/A) (DoD) The System Administrator and ERP Administrator will ensure authentication credentials or sensitive data are stored in encryption using FIPS 140-2 compliant encryption, NIST Certified cryptography or NSA approved cryptography depending on the classification of the data residing within the application.*

### **3.10.2 In transit – Network connections to the application**

When an ERP application connection is requested via the network, the client should provide an individual account name and authentication credentials to access the database. The ERP application account name and any password transmission from a client to a database server over a network must be encrypted. Encrypting information reduces the risk of unauthorized access to the data while being transmitted. The interception and/or disclosure of highly sensitive data, could cause loss of business, lawsuits and identify theft.

- *(ERP007600: N/A) The System Administrator and ERP Administrator will ensure the transmission of an ERP account name and password from a client to an ERP Application server over a network is encrypted using NIST-certified cryptography.*
- *(ERP007700: N/A) The System Administrator and ERP Administrator will ensure all network connections to an ERP application require an individual ERP application account and authentication credentials. Classified data transmitted through a network that has cleared to a lower level than the data being transmitted are separately encrypted using NSA-approved cryptography.*
- *(ERP007800: N/A) The System Administrator and ERP Administrator will ensure file encryption, VPN, SSH and other entities to be encrypted are FIPS 140-2 compliant.*
- *(ERP007900: N/A) (DoD) The System Administrator and ERP Administrator will ensure the application does not send e-mail messages that include executable code.*
- *(ERP008000: N/A) (DoD) ERP Administrator will ensure the application does not transmit unsigned CAT 1 or CAT 2 mobile code.*
- *(ERP008100: N/A) (DoD) The System Administrator and ERP Administrator will ensure the application does not transmit mobile code that attempts to access local operating system resources or establish network connections to servers other than the application server.*
- *(ERP008200: N/A) (DoD) The System Administrator and ERP Administrator will ensure the application does not execute mobile code without requiring and validating digital signatures.*

- *(ERP008300: N/A) (DoD) The System Administrator and ERP Administrator will ensure the application does not utilize any type of mobile code for which there is no established policy.*

### **3.11 Application Access to System Services**

Accounts created for and used by non-interactive automated processing are subject to special consideration. These database accounts may be used for a variety of functions such as maintenance batch jobs, etc. These accounts will not be shared with interactive application users. The primary vulnerability with non-interactive accounts is a frequent requirement to store the account name and password within application code, external files, or even on a remote server (example- 3<sup>rd</sup> party business warehouse application) and the possibility of exposure of this information during the logon process. Assignment of the minimal level of authorization access is critical for this reason. Accounts used for automated processing should be restricted to appropriate hours of access where possible.

- *(ERP008310: N/A) The IAO and ERP Administrator will ensure non-interactive automated processing accounts meet the same security requirements as application dialog userids with the exception of password lifetime.*
- *(ERP008320: N/A) The ERP Administrator will ensure the use of non-interactive automated processing accounts is documented and authorized by the IAO.*
- *(ERP008330: N/A) The ERP Administrator will ensure application utilities and batch submissions do not contain or store unencrypted database account names and passwords.*
- *(ERP008500: N/A) (DoD) The IAO and ERP Administrator will ensure the application process removes temporary objects from memory or disk before the application terminates.*

### **3.12 Application Access to Database Services**

- *(ERP008400: N/A) (DoD) The IAO and ERP Administrator will ensure the application does not modify data files outside the scope of the application.*

#### **3.12.1 Separation of user interface from data storage**

User data will be stored in different directory than application code to prevent any compromise in information. User credentials will be deleted from a client computer immediately upon session termination in order to prevent an unauthorized individual from gaining access to the ERP application on a recently used client computer.

- *(ERP008600: N/A) (DoD) The ERP Administrator will ensure the application code and application data is not located in the same directory.*
- *(ERP008700: N/A) (DoD) The ERP Administrator will ensure the application does not store authentication credentials on client computers after a session terminates.*

### 3.13 Application Configuration and Customization Requirements

Delivered application and security should be customized to comply with governing policies and standards. Management, data owners, IAO, ERP Administrator, SA and other stakeholders should all work together to customize the system to match said governing policies and standards.

- *(ERP008900: N/A) (DoD) The ERP Administrator and developers will ensure the application does not include an explicit error and exception handling capability. Application error and exception messages displayed to users reveal information that could be utilized in a subsequent attack.*
- *(ERP009000: N/A) (DoD) The ERP Administrator and System Administrator will ensure the application interfaces are identified and protected.*
- *(ERP009100: N/A) (DoD) Developers will ensure the application code does not contain invalid references to network resources (pathnames, URLs, etc).*

All files, ERP application accounts, application objects and application code that are solely associated with an unused module or area of the ERP application should be removed from the ERP application, however, based on the very large number of transactions and programs, mitigating controls will be used instead.

- *(ERP001400: N/A) (DoD) The IAO will not grant access to transactions or authorization objects not being used for a defined purpose.*

### 3.14 Patching and Maintenance Requirements

ERP patches are identified and sent out by the vendor. At that point in time the ERP Administrator should plan a system outage in order to apply the patch to the ERP application.

Maintenance includes upgrades, and test system refreshes with production data. Upgrades should be performed in a timely manner in order to maintain support from the vendor. This task should be performed as a project plan and executed by IAO, ERP Administrators, Developers and any necessary Application Users. Testing should take place by all groups in order to assure integrity of the system after the upgrade. Sign off should occur by the governing body indicating that they agree that the integrity of the system is intact and ready to be moved to production.

Test System refreshes should be scheduled on a quarterly basis. The SA schedules downtime for the refresh and works together with the IAO and users to accomplish this task. Even though this only affects the test system, testing should be performed after the refresh in order to assure system integrity is intact.

- *(ERP009200: N/A) (DoD) The ERP Administrator will ensure the application is tested for buffer overflows.*

### 3.15 Audit

The purpose of these reviews is to ensure no one is attempting to gain unauthorized access by guessing passwords and that any unauthorized transaction attempts are mistakes and not malicious. Auditing will be configured and implemented on all systems. Auditing is capable of capturing all ERP Application operations, including application events, modification to database parameters and resources as well as modification to the data. Auditing can result in a great deal of information being collected on ERP Application activities. There should be a determination made of critical events/data to audit to allow enough granularity to allow for the monitoring of intrusive activity.

Logging and monitoring should exist for tables, which are deemed critical, and for powerful transactions and authorization objects.

Controls should be in place to ensure audit log data have not been deliberately or accidentally disabled. If this is not done there is a risk that logging would not be done and an attack could remain undetected.

- *(ERP009300: N/A) (Industry) The ERP Administrator and IAO will ensure all updates to security software or security functionality of software and applications is logged.*
- *(ERP009400: N/A) (DoD) The ERP Administrator will ensure the IAO is notified when the application logs are near capacity.*
- *(ERP009500: N/A) The ERP Administrator and IAO will ensure the activities of administrators are monitored for evidence of misuse of privileges.*

Controls will be in place to ensure audit log data is protected from corruption or deletion. This control is necessary to ensure audit log data is protected. Without protection, the data could be changed or deleted intentionally or unintentionally, rendering the data inaccurate or unavailable for investigative purposes.

- *(ERP009600: N/A) (DoD) The ERP Administrator will ensure logs are maintained for audit purposes are stored securely to not be vulnerable to unauthorized deletion, modification or disclosure.*
- *(ERP009700: N/A) (Industry) The IAO will ensure use of system audit tools are restricted to authorized users.*
- *(ERP009710: N/A) (DoD) The IAO will ensure ERP Application audit data is captured and maintained for one year.*

Controls should be in place to obtain a list of the “administrative user” userids and then ensure the appropriate logging of these userids is taking place. Monitoring for evidence of misuse helps to protect the integrity and availability of the system.

- *(ERP009900: N/A) The IAO will review “Authorization to Maintain Security” audit logs once a month to ensure no one other than the IAO has access to modify security.*
- *(ERP010000: N/A) The IAO will ensure changes to identifiers and role privileges or attributes are logged.*

The security audit log will be reviewed on a regular basis. Failure to monitor the system to detect unauthorized activities and reconciliation of abnormalities could result in unauthorized disclosure, modification or destruction of data.

- *(ERP010100: N/A) The IAO will ensure security violations are reviewed and reconciled based on the access requirements and security needs of each individual.*
- *(ERP010200: N/A) The IAO and ERP administrator will review the Systems periodically to ensure compliance with security controls*

The IAO will conduct security audit reviews on all production systems. All reviews are documented in the corresponding review record. The IAO should become familiar with SOX and HIPPA audit requirements in order to monitor and review activity to ensure users are set up appropriately to satisfy these requirements.

- *(ERP010300: N/A) IAO will review “changes to access in production systems” once a month to ensure no roles have been changed in a production system.*
- *(ERP010400: N/A) IAO will review access to “View System Logs” once a month to ensure no one other than the users with batch submit access can display the system log.*
- *ERP010500: N/A) IAO will review “authorization to process batch input sessions” once a monthly to ensure only authorized userids have access to delete, release and lock sessions.*
- *(ERP010600: N/A) IAO will review “batch and generic userids” once a month in order to ensure all such userids are valid and that no new userids have been created without approval. All Anomalies are reviewed and appropriate action taken to secure the system.*
- *(ERP010700: N/A) IAO will review access to the “background administrator function” once a month to ensure only appropriate userids have this ability.*
- *(ERP010800: N/A) IAO will review access to “system administration functions (ERP Administrator)” once a month in order to ensure only appropriate userids have these abilities.*
- *(ERP010900: N/A) IAO will review “data dictionary functions” once a month to ensure only appropriate userids have this ability.*
- *(ERP011000: N/A) IAO will review administrator access to the transport and change system once a month in order to ensure all such userids are valid.*

- *(ERP011100: N/A) IAO will review “developer access” once a month in order to ensure only appropriate userids have this access.*
- *(ERP011200: N/A) Users that have been inactive for a period of 60 consecutive days are disabled.*
- *(ERP011300: N/A) Users will be deleted and purged from the access control system after 120 days of consecutive inactivity.*
- *(ERP011400: N/A) IAO will review “locked or inactive userids” once a month in order to ensure all userids that are inactive for over 30 days have their user group set to “UNUSED IDS”.*
- *(ERP011500: N/A) IAO will review “system parameters” once a month to ensure applicable system parameters comply with standards and that changes to system parameters are documented and appear appropriate. This includes auditing of creating, alteration or deletion of application objects, granting and revoking of roles/privileges, connection failures, changes to classified data, unusual patterns of activity, configuration changes, critical table changes.*
- *(ERP011600: N/A) IAO will review a “list of conflicting access” once a month in order to ensure all such userids have a valid approval by the appropriate approver(s) and that segregation of duties is intact for SOX audit information.*
- *(ERP011610: N/A) IAO will ensure access to personal and personnel data has been approved by the data owner and is appropriate access for a given user to perform their job function. This is done to satisfy HIPPA requirements.*

### **3.16 Backup**

ERP systems will be included in the enclave backups as described in the Enclave STIG.

## **APPENDIX A. RELATED PUBLICATIONS**

Department of Defense (DoD) Directive 8500.1, "Information Assurance (IA)," October 24, 2002

Department of Defense (DoD) Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

Chairman Of The Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) And Computer Network Defense (CND)," 25 March 2003

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements For Cryptographic Modules" May 25, 2001 as modified December 3, 2002. This publication may be found on the NIST website <http://www.nist.gov>.

The Expert Guide to PeopleSoft Security. Copy Write 2004, Jason D. Carter, MS author.

Security, Audit and Control Features- SAP R3- A Technical and Risk Management Reference Guide, 2002, IT Governance Institute

This page is intentionally left blank.



## APPENDIX B. GLOSSARY OF TERMS

TERM	DEFINITION
	.

This page is intentionally left blank.

## APPENDIX C. LIST OF ACRONYMS

ACRONYM	PLAIN TEXT
ERP	Enterprise Resource Planning
COTS	Commercial Off the Shelf
IA	
IT	Information Technology
STIG	Security Technical Implementation Guide
DoD	Department of Defense
MAC	Mandatory Access Control
CRM	Customer Relations Management
IAO	Information Assurance Officer
SA	System Administrator
NSO	Network Security Officer
DBA	Database Administrator
IAM	Information Assurance Manager
CCB	Change Control Board
DAA	Designated approving Authority
SDID	Short Description Identifier
PDI	Potential Discrepancy Item
IAVM	Information Assurance Vulnerability Management
JTF-GNO	Joint Task Force-Global Network Operations
IASE	Information Assurance Support Environment
AIS	Automated Information Systems
HR	Human Resource
QA	Quality Assurance
NIST	
FIPS	
PKI	Public Key Infrastructure
SAMI	
VPN	Virtual Private Network
SSH	Secure Shell

This page is intentionally left blank.